DEPUTY ATTORNEY GENERAL ROD J. ROSENSTEIN DELIVERS KEYNOTE ADDRESS AT GEORGETOWN UNIVERSITY LAW CENTER'S CYBERCRIME 2020 CONFERENCE

1 message

USDOJ-Office of Public Affairs <USDOJ-OfficeofPublicAffairs@public.govdelivery.com> Thu, Nov 29, 2018 at 1:23 PM
Reply-to: USDOJ-OfficeofPublicAffairs@public.govdelivery.com
To: kevin.collier@buzzfeed.com

DEPUTY ATTORNEY GENERAL ROD J. ROSENSTEIN DELIVERS KEYNOTE ADDRESS AT GEORGETOWN UNIVERSITY LAW CENTER'S CYBERCRIME 2020 CONFERENCE

Washington, D.C.

Our mission is to protect the public, defend our nation, and prevent nascent threats from blossoming into full-blown perils, while upholding the rule of law and maintaining the public's trust and confidence.

We encourage the private sector and academia to join us in addressing these challenges. A better common understanding of emerging threats facilitated by new technology can help tech companies develop safer, more secure software and devices. It will allow consumers to make more deliberate decisions about the tradeoffs they make every day between convenience and security.

Remarks as prepared for delivery

Good afternoon. It is a pleasure to join you today. I always enjoy visiting the Georgetown University Law Center. For many years I helped to teach a trial advocacy seminar here for practicing lawyers.

I am grateful to Professor [Laura] Donohue, for the introduction, and to Georgetown for co-hosting today's event with the Department of Justice. Jointly sponsoring thoughtful public forums is an excellent way to highlight important legal issues and spur an exchange of ideas among representatives of the government, private sector, and academia.

None of us has all the answers, and each of us may bring different perspectives about the nature of our problems and the need for answers.

There is a story about a man who went to a pet shop to buy a birthday gift for his mother. The mother lived alone, and the son thought it would be nice to give her a pet as a companion. The shop owner recommended a parrot. Not just any parrot. A special parrot. He said, "This

parrot is fluent in English." The man thought that would keep his mother entertained, so he bought it and arranged for delivery.

About a week later, the man received a thank-you note. It said “Son, I am so grateful that you sent that wonderful bird. I cooked it and ate it for dinner. It was delicious!”

The man was horrified. He called his mother immediately. "Why did you eat the parrot?" he asked. “That parrot was so talented that it could speak English fluently!"

His mother replied, "Well, then it should have said something!"

And the moral of the story is, if you don’t talk when you get the chance, don’t complain later!

Our symposium topic – the future of cybercrime – certainly warrants a thoughtful dialogue. Cybercrime is a priority for the Department of Justice.

Attorney General Jeff Sessions established a Cyber-Digital Task Force earlier this year to answer two questions: what are we doing to address cyber threats, and how can we do better? The Task Force released a comprehensive report a few months ago. The report describes the multi-faceted challenges of cyber-enabled crime, including the need to develop strategies to detect, deter and disrupt threats; inform victims and the public about dangers; and maintain a skilled workforce.

This symposium takes a similar approach. By posing the right questions about technology, we can focus on getting the right answers. How do technological innovations facilitate crime and create new law enforcement challenges? Do our laws adequately address the new obstacles? And how do we — collectively, the public and private sectors —better anticipate and address the unprecedented challenges that new technologies create?

Our mission is to protect the public, defend our nation, and prevent nascent threats from blossoming into full-blown perils, while upholding the rule of law and maintaining the public’s trust and confidence.

We encourage the private sector and academia to join us in addressing these challenges. A better common understanding of emerging threats facilitated by new technology can help tech companies develop safer, more secure software and devices. It will allow consumers to make more deliberate decisions about the tradeoffs they make every day between convenience and security.

In keeping with the theme of today’s symposium, I’d like to share some thoughts about technology and security. And by “security” I mean both cybersecurity and security in the traditional sense of public safety.

Our generation benefits from amazing technological developments. Things that were literally unimaginable in my youth are taken for granted by my children. But the people who create and market new tools often do not consider all of the implications for public safety – how innocent users can be victimized by new technology, and how malicious users can misuse new technology. That is not their job. It should be somebody’s job. At the Department of Justice, we accept it as part of our job.

For example, people now store sensitive and valuable information on electronic devices. Hackers can not only steal the information, they can disable and destroy the devices.

Companies collect tremendous amounts of information about their customers. Some users do not understand that the companies use that data for commercial advantage. And all users are vulnerable when criminals steal the data, and employ it victimize them in fraud schemes.

Social media platforms provide unprecedented opportunities for the free exchange of ideas. But many users do not understand that the platforms allow malicious actors, including foreign government agents, to deceive them by launching vast influence operations.

In the near future, we will need to come to terms with “deep fake” videos, which will challenge our confidence that we can rely even on what we see with our own eyes and hear with our own ears.

Technology is advancing at a speed and volume that exceeds the capacity of most people to comprehend the accompanying risks, let alone to protect against them. We need technology companies and communications providers to accept responsibility for developing routine business practices that account for all the ways their products may be misused. And we need government agencies to develop investigative capabilities that keep up with enforcement challenges.

We should anticipate that criminals will deploy smarter, adaptive malware capable of thwarting existing defenses. They will use impenetrable communications platforms that defeat our ability to detect and prevent crimes.

Finding ways to forestall those ominous consequences will require that we take at least three steps:

- First, we must place security on the same footing as novelty and convenience, and design technology accordingly, in the same way that we design automobiles with horns, emergency lights, seatbelts and airbags; we equip ships with lifeboats and floatation devices; and we construct high-rise buildings with sprinklers and fire escapes. Anticipating worst-case scenarios needs to be part of the development process.
- Second, we need the private sector to coordinate with law enforcement agencies about emerging security issues, and work cooperatively to address them.
- Finally, we must acknowledge that thwarting harmful, destructive activities enabled by technology is a moral imperative, and that helping law enforcement accomplish that goal is in society’s best interest. We cannot accept a culture in which technology companies work to defeat legitimate law enforcement activities.

I want to make clear that I and my government colleagues appreciate, value, and support technological progress. Technology spawns incredible advances. It exponentially expands human knowledge, tremendously improves health and safety, and dramatically enhances our quality of life.

But technology is not intrinsically good or bad. Like a knife, or a hammer, it is merely a tool. It can be used to accomplish something amazing — such as the creation of a life-saving medical device — or something awful. Consider the creation and distribution of child pornography, or the spread of malware capable of disabling devices that contain all the details of our lives, just as a fire can destroy a home and vanquish a lifetime of mementoes.

When the Department of Justice and Georgetown first partnered to sponsor a cybercrime symposium in 2014, a panel of technologists anticipated the threat posed by a novel use of malware to extort victims by encrypting their data and holding it for ransom. They unanimously declared ransomware the threat of the future. They were right.

By 2016, ransomware emerged as a top threat worldwide, indiscriminately attacking small businesses, law firms, government offices, and hospitals. In 2017, it caused an international panic, as the WannaCry and NotPetya ransomware attacks swept the globe. Exploiting our dependency on data was a technological innovation in cybercrime and a novel business model. Ransomware caused an estimated $5 billion of damage last year.

Without a concerted effort to to alter our trajectory, the malicious use of technology will be more pernicious and pervasive tomorrow than it is today, and even more difficult to combat.

During my lifetime, the technology sector has grown from almost nothing to play a central role in our lives. The growth and profitability of the tech sector is enhanced by quick, bold moves. Being the first to market a new technology is the goal of every tech company. A company that develops a "killer app" or the next must-have household device can achieve market dominance almost overnight. Consider Twitter. In just five years, between 2010 and 2015, the Twitter community of users exploded from 30 million to over 300 million worldwide, making it one of the most influential communications providers on the planet.

The market quickly rewards novel benefits. Unintended adverse consequences often emerge only over time.

Building secure devices requires additional testing and validation—which slows production times — and costs more money. Moreover, enhanced security can sometimes result in less user-friendly products. It is inconvenient to type your zip code when you use a credit card at the gas station, or type a password into your smartphone.

Creating more secure devices risks building a product that will be later to market, costlier, and harder to use. That is a fundamental misalignment of economic incentives and security.

Other misalignments impacting security and accountability also exist. Consider "Internet of Things" technologies, which some call IoT. In 2016, a botnet of IoT devices was used to launch the largest distributed denial-of-service or "DDoS" attack ever. The attack originated from thousands of IoT devices infected with "Mirai" malware. Unlike other malware, the Mirai was written specifically to infect IoT devices. It turned these everyday products into an army of devices capable of transmitting torrents of Internet traffic capable of knocking targeted networks offline.

A Mirai attack against a well-known blogger's website frequently targeted by DDoS attacks was 35 times larger than anything the website had ever suffered before. And one day in October 2016, thousands of Mirai-infected IoT devices unleashed a torrent of traffic that overwhelmed an internet-services company. Many high-traffic websites that relied on the company were inaccessible for substantial periods of the day.

Fortunately, FBI and DHS agents identified and arrested the creators of the Mirai malware, and they pleaded guilty last year.

The Mirai botnet was targeted IoT devices with poor security features. According to one security researcher, an estimated 500,000 IoT devices can be hijacked using default username/passwords pairs. Keep in mind that the Mirai malware exploited just tens of thousands of devices.

We depend on technology, but technology that lacks security can be a menace, and market forces do not require companies to anticipate and prevent misuse of their products.

The talent and capacity for improving cybersecurity, thwarting cyber threats, and improving our security posture is distributed across the private and public sectors. No one should be under the illusion that law enforcement alone is the answer to resolving these challenges.

But law enforcement is a part of the solution. You cannot deter malicious uses of technology without having a credible capacity to impose punishment for committing fraud, hacking into information systems, stealing data, and disabling computers.

The ability to attribute the source of an attack or intrusion is critical to law enforcement's ability to help. It is impossible to employ criminal enforcement tools and other forms of retribution without first identifying the perpetrators – whether they are ordinary criminals, transnational organized criminal organizations, or hostile nation-state officers. Law enforcement agencies work with intelligence community partners to play a major role in identifying who is responsible for cyber violations.

Apart from battling cyber threats, technology also influences other crime-fighting efforts. Our ability to gather electronic evidence increasingly relies on remote communications service providers and device manufacturers.

Multiple factors drive those companies' decisions. Companies are in the business of generating profits. I do not blame them for failing to consider law enforcement and public safety concerns. But when you hear corporate leaders complain about law enforcement demands, it is important to understand that what is good for a technology company in terms of bottom-lie profits is not necessarily good for America. Their interests are not always aligned with yours.

Much of what they do to earn money does provide great public benefits. But economic competitiveness in global markets is not informed by general concerns about public good. Furthermore, some communications providers chronically understaff their offices that respond to legal process from law enforcement. In some cases, the lack of personnel causes lengthy delays in producing evidence, even when production is ordered by a court.

The impact of their decisions on law enforcement's ability to investigate crimes and enforce laws is far-reaching, because electronic evidence held by third parties is now essential to many types of investigations.

Pedophiles teach each other how to evade detection on darknet message boards. Gangs plan murders using social media apps. And extortionists deliver their demands via email. So, it is important for those of us in law enforcement to raise the alarm and put the public on notice about technological barriers to obtaining electronic evidence.

One example of such a barrier is "warrant-proof" encryption, where tech companies design their products or services in such a way that they claim it is impossible for them to assist in the execution of a court-authorized warrant. These barriers are having a dramatic impact on our cases, to the significant detriment of public safety. Technology makers share a duty to comply with the law and to support public safety, not just user privacy.

It is not inconsistent to value both securing devices against illegal intrusions and providing lawful access with judicial orders. Obviously the strongest possible encryption would be impregnable even to law enforcement officers with court orders, but responsible encryption is achievable, and in certain contexts it already exists. We encourage technology companies to develop "responsible encryption" — effective, secure encryption that resists criminal intrusion but allows lawful access with judicial authorization.

As an analogy, we require buildings to disable elevators in the event of a fire, but we also expect them to retain the capacity for firemen to use them in an emergency. Whatever structures we build, whether physical or virtual, someone always should have the ability to access it in an emergency, but the key does not need to be held by a single entity, and it does not need to be held by the government.

Law enforcement's efforts to preserve the ability to gather court- electronic evidence with court authorization are sometimes met with mistrust, skepticism, and derision. Some in the tech community and academia have responded dismissively to the problem of law enforcement's diminishing ability to collect evidence, claiming that law enforcement will find other ways of solving many crimes.

But in many cases, we will not find other ways to solve crimes. And in other cases, we may be able to get the evidence we need eventually, but it may be a great cost in terms of harm to future victims, and expense to government agencies. Improvements in the ability to investigate crime and hold perpetrators accountable must match the pace at which technology is making crimes easier to commit, and more destructive.

Some technology experts castigate colleagues who engage with law enforcement to address encryption and similar challenges. Just because people are quick to criticize you does not mean that you are doing the wrong thing.

There is nothing virtuous about refusing to help develop responsible encryption, or in shaming people who understand the dangers of creating any spaces – whether real-world or virtual – where people are free to victimize others without fear of getting caught or punished.

I recently came across an article about Ray Ozzie, a noted technologist who once served as Microsoft's chief technical officer as well as its chief software architect. On his own initiative, Ozzie reportedly developed a system that he believes could allow law enforcement access to encrypted data without significantly increasing security risks for users.

I do not know whether that system works, but I applaud everyone who works constructively on solutions to the challenge of providing security against criminal intrusions without eliminating protection by law enforcement. We should not let ideology or dogma stand in the way of constructive academic engagement. The technologists, cryptographers, and researchers working on this problem recognize that law enforcement has a duty to pursue solutions to these problems, so that we can do the job the public expects us to do – promote justice, protect public safety, deter crime, and punish criminals.

I encourage security researchers, technology companies, academics, information security professionals, and others in the private sector to keep searching for constructive solutions that will enable us to harness the wonder of new advances without descending into technological anarchy.

I am grateful to Georgetown Law School for joining with the Department of Justice to provide a forum for discussing these important issues.

Thank you very much.

# # #

DAG

18-1572

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.